LEI Nº 8847, DE 24 DE OUTUBRO DE 2025

Estabelece diretrizes para a implementação de uma Política Estadual de Prevenção e Combate a Fraudes Virtuais e Crimes Cibernéticos no âmbito do estado do Piauí.

O GOVERNADOR DO ESTADO DO PIAUÍ , Faço saber que o Poder Legislativo decreta e eu sanciono a seguinte Lei:

Art. 1º Ficam estabelecidas, no âmbito do estado do Piauí, as diretrizes para a formulação e implementação da Política Estadual de Prevenção e Combate a Fraudes Virtuais e Crimes Cibernéticos, observando-se, entre outros diplomas, a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a Lei nº 14.155, de 27 de maio de 2021 (que altera o Código Penal para tipificar e agravar penas de crimes cibernéticos), bem como demais legislações correlatas que tratem da repressão a ilícitos praticados por meios digitais.

Art. 2º Para os fins desta Lei, consideram-se fraudes virtuais e crimes cibernéticos as condutas ilícitas, praticadas por meio de redes digitais, dispositivos eletrônicos, sistemas informatizados ou tecnologias emergentes, incluindo, entre outras, as seguintes:

I - **phishing**: prática fraudulenta que consiste no envio de mensagens eletrônicas, geralmente por e-mail ou por meio de páginas falsas na internet, com o objetivo de induzir a vítima a fornecer dados pessoais, bancários, senhas ou outras informações sensíveis, simulando comunicações legítimas de instituições conhecidas, em violação ao disposto no Código Penal, com redação dada pela Lei nº 14.155, de 27 de maio de 2021;

II - **smishing**: modalidade de fraude eletrônica semelhante ao **phishing,** mas realizada por meio de mensagens de texto (SMS) ou aplicativos de mensagens instantâneas, visando obter dados sigilosos, instalar programas maliciosos ou induzir a vítima a acessar **links** fraudulentos;

III - **vishing**: forma de golpe que utiliza chamadas telefônicas, incluindo ligações via aplicativos de voz sobre IP (VoIP), para obter informações pessoais ou financeiras da vítima, mediante engenharia social, uso de informações prévias e, muitas vezes, simulação de autoridades ou representantes de empresas legítimas;

IV - **malware**: termo genérico para designar softwares maliciosos desenvolvidos para danificar, explorar ou obter acesso não autorizado a sistemas, redes ou dispositivos, incluindo, entre outros, vírus, **worms, trojans, spyware e adware**;

V - **ransomware**: tipo específico de malware que criptografa dados ou bloqueia o acesso a sistemas, exigindo pagamento de resgate para restabelecimento do acesso, conduta tipificada pelo Código Penal, com alterações da Lei nº 14.155/2021;

VI - **spoofing**: técnica utilizada para falsificar informações de identificação, como endereços de e-mail, números de telefone ou endereços IP, a fim de enganar a vítima e fazê-la acreditar que está se comunicando com uma fonte legítima;

VII - engenharia social: conjunto de técnicas de manipulação psicológica utilizadas para induzir uma pessoa a revelar informações confidenciais ou executar ações que comprometam a segurança de sistemas e dados, explorando vulnerabilidades comportamentais;

VIII - **deepfake** malicioso: criação, manipulação ou alteração digital de imagens,

vídeos ou áudios utilizando inteligência artificial ou tecnologias similares, com o objetivo de difamar, ameaçar, chantagear, extorquir, induzir erro ou causar dano moral, patrimonial ou à honra da vítima;

IX - assédio virtual (**cyberbullying**): prática de hostilizar, ameaçar, humilhar, constranger ou perseguir pessoa por meio de tecnologias de informação e comunicação, de forma reiterada ou não, causando-lhe dano psicológico, emocional, reputacional ou social, podendo, em casos graves, induzir ou instigar a vítima a atentar contra a própria vida;

X - **botnet**: rede de dispositivos infectados por **malware,** controlados remotamente por um agente malicioso, utilizada para executar ações em massa, como ataques distribuídos de negação de serviço (DDoS), envio de **spam** ou disseminação de outros **malwares**;

XI - ataque de negação de serviço (DoS/DDoS): ação que visa sobrecarregar um sistema, servidor ou rede, tornando-o indisponível para usuários legítimos, geralmente utilizando tráfego massivo oriundo de múltiplas fontes;

XII - **keylogger**: **software** o u **hardware** que registra, de forma oculta, as teclas digitadas por um usuário, com o intuito de capturar senhas, dados bancários ou outras informações sigilosas;

XIII - **credential stuffing**: método de ataque em que credenciais (usuário e senha) obtidas de vazamentos anteriores são testadas de forma automatizada em diversos sistemas e serviços, visando acessar contas de forma ilícita;

XIV - divulgação não consentida de conteúdo íntimo **(revenge porn)**: exposição, compartilhamento ou comercialização de imagens, vídeos ou áudios de cunho sexual ou privado, com ou sem manipulação digital, sem o consentimento da vítima, prática também conhecida como **revenge porn**, em violação à sua intimidade, privacidade e dignidade, independentemente de motivação pessoal, econômica ou emocional;

XV - roubo ou falsificação de identidade digital: uso indevido de dados, credenciais, perfis ou contas de terceiros para obter vantagens ilícitas, prejudicar a reputação da vítima ou cometer outros crimes.

Art. 3º A Política Estadual de Prevenção e Combate a Fraudes Virtuais e Crimes Cibernéticos como objetivos:

I - estimular a integração e a cooperação entre órgãos de segurança pública, Ministério Público, Poder Judiciário, órgãos de defesa do consumidor, instituições de ensino, setor privado e sociedade civil, visando à prevenção, identificação e combate de fraudes virtuais e crimes cibernéticos, respeitada a competência de cada ente e instituição;

II - favorecer o desenvolvimento, a difusão e a adoção de tecnologias seguras e mecanismos de proteção digital por usuários, empresas e instituições, com ênfase na prevenção de fraudes e na redução de vulnerabilidades;

III - colaborar com ações e iniciativas que ampliem a capacidade de resposta a incidentes de segurança digital, priorizando a mitigação célere de danos e a restauração de serviços afetados, sempre que possível por meio de parcerias e cooperação técnica;

IV - estimular a educação digital voltada à proteção de dados pessoais, à privacidade e à cidadania digital, em consonância com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

V - assegurar que as medidas de prevenção e combate respeitem os direitos e garantias fundamentais previstos na Constituição Federal, no Marco Civil da Internet (Lei nº 12.965/2014) e nas demais normas aplicáveis;

VI - facilitar a cooperação técnica entre o Estado e entidades públicas ou privadas objetivando o fortalecimento das estratégias de prevenção e combate a ilícitos cibernéticos;

VII - favorecer o desenvolvimento de projetos e pesquisas voltados à criação de soluções tecnológicas inovadoras para segurança da informação e prevenção de crimes digitais, respeitadas as diretrizes de proteção de dados e propriedade intelectual;

VIII - buscar integração com programas nacionais e internacionais voltados à cibersegurança e à cooperação no combate a crimes digitais;

IX - desenvolver ações específicas de conscientização e prevenção contra crimes

cibernéticos cometidos mediante uso indevido de inteligência artificial, com foco na proteção de crianças, adolescentes, idosos e demais grupos vulneráveis, abrangendo a prevenção da pornografia infantil **deepfake** e de qualquer conteúdo digital gerado artificialmente que viole a dignidade e a integridade desses grupos.

Art. 4º A implementação da Política Estadual de Prevenção e Combate a Fraudes Virtuais e Crimes Cibernéticos observará, entre outros, os seguintes princípios:

I - proteção integral da privacidade e dos dados pessoais, assegurando que todas as ações estejam em conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), o Marco Civil da Internet (Lei nº 12.965/2014) e demais normas de tutela da intimidade, honra e imagem;

II - proporcionalidade e razoabilidade na adoção de medidas de prevenção, monitoramento e combate, de forma que as ações sejam limitadas ao estritamente necessário para o interesse público e gravidade da conduta;

III - transparência ativa e passiva na divulgação de diretrizes, relatórios e resultados das ações implementadas no âmbito da Política, observados os sigilos legalmente protegidos, como o sigilo de comunicações, o sigilo bancário e o sigilo fiscal;

IV - cooperação técnica, institucional e informacional entre órgãos e entidades públicos e privados, respeitando a legislação vigente, tratados e acordos multilaterais de que o Brasil seja signatário, bem como a proteção da soberania e da segurança nacional;

V - prioridade de proteção a grupos em condição de maior vulnerabilidade, como crianças, adolescentes, idosos, pessoas com deficiência e populações em situação de risco social, com adoção de estratégias de comunicação e prevenção adaptadas a cada realidade;

VI - neutralidade e adaptabilidade tecnológica, garantindo que as disposições da presente Política sejam aplicáveis a quaisquer sistemas, dispositivos, plataformas ou recursos tecnológicos, atuais ou futuros, prevenindo obsolescência normativa diante da rápida evolução digital;

VII - respeito à cadeia de custódia e à integridade das evidências digitais, assegurando que a preservação, coleta, armazenamento e análise de dados para fins de apuração de crimes cibernéticos se deem em conformidade com os padrões técnicos e jurídicos vigentes.

Art. 5º Para viabilizar a execução desta Política, o Poder Executivo poderá, observados os limites de sua competência, interesse e conveniência, em articulação com órgãos e entidades competentes, públicas e privadas:

I - firmar convênios, termos de cooperação e parcerias visando à promoção de campanhas de prevenção e conscientização sobre fraudes virtuais e crimes cibernéticos;

II - estimular e facilitar treinamentos e capacitações especializadas para agentes públicos e privados envolvidos na prevenção, identificação e combate a ilícitos digitais;

III - apoiar, direta ou indiretamente, projetos de pesquisa e desenvolvimento nas áreas de cibersegurança, inteligência artificial aplicada à segurança digital e análise forense computacional;

IV - fomentar a criação, aprimoramento ou manutenção de canais de denúncia acessíveis, seguros e compatíveis com padrões de proteção de dados, para uso por vítimas ou testemunhas de crimes cibernéticos.

Art. 6º **VETADO.**

Art. 7º O Poder Executivo regulamentará esta Lei, no que couber, definindo os órgãos e entidades responsáveis pela coordenação, execução, monitoramento e avaliação das ações previstas, bem como os procedimentos, critérios e prazos para sua implementação, podendo, para tanto, firmar parcerias, convênios e termos de cooperação com instituições públicas e privadas, observada a legislação vigente.

Art. 8º Esta Lei entra em vigor na data de sua publicação.

PALÁCIO DE KARNAK, em Teresina (PI), 24 de outubro de 2025.

(*assinado eletronicamente*)
RAFAEL TAJRA FONTELES
Governador do Estado do Piauí

(*assinado eletronicamente*)
IVANOVICK FEITOSA DIAS PINHEIRO
Secretário de Governo

(*) Lei de autoria do Deputado Dr. Rubens Vieira, PT (informação determinada pela Lei nº 5.138, de 07 de junho de 2000, alterada pela Lei 6.857, de 19 de julho de 2016)

Documento assinado eletronicamente por **RAFAEL TAJRA FONTELES**, **Governador do Estado do Piauí**, em 30/10/2025, às 19:02, conforme horário oficial de Brasília, com fundamento no Cap. III, Art. 14 do Decreto Estadual nº 18.142, de 28 de fevereiro de 2019.

A autenticidade deste documento pode ser conferida no site https://sei.pi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0020858611** e o código CRC **F31C239E**.

Referência: Caso responda este Documento, indicar expressamente o Processo nº 00010.013501/2025-01

SEI nº 0020858611